RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: LAB1-R05

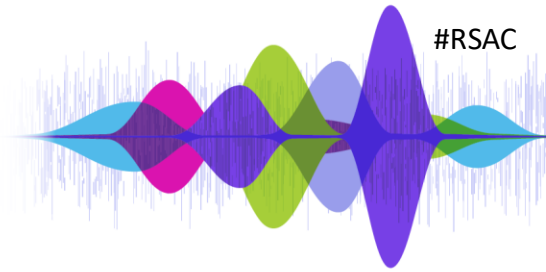
Physical Breaches, Digital Consequences: Testing Physical Threat Vectors

Ana Aslanishvili

Founder & CEO
Pine Risk Management
linkedin.com/in/anauthorized

Shawn Abelson

Founder & COO
Pine Risk Management
linkedin.com/in/shawn-abelson



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

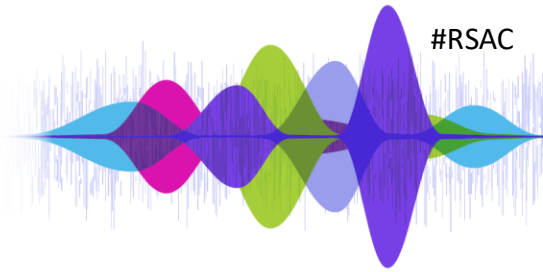
Nothing discussed or taught during this course should be construed, considered, or interpreted as legal advice. We are not lawyers, and we're definitely not your lawyers.
You must get permission before red teaming, otherwise it is a crime. There is no physical security bug bounty program.
Cybersecurity and Physical Security are separate professions. Knowledge of one does not equate to knowledge in the other.

Agenda

Professional

Technical

Foundation



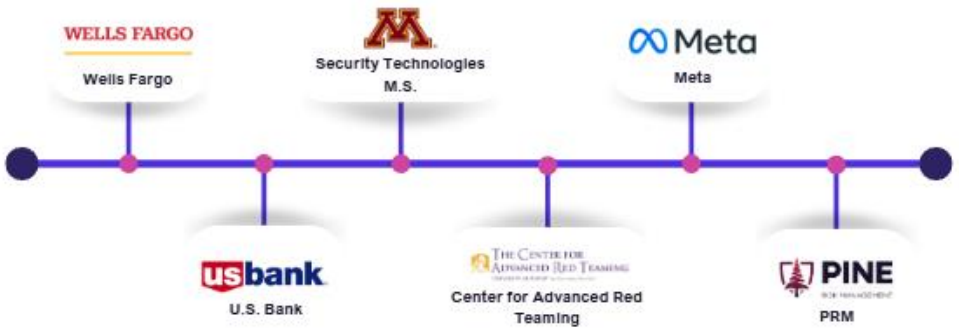
Agenda

- 1. Foundations of Physical Red Teaming
- 2. Threat Ideation Exercise
- 3. Physical TTPs: Demo Time
- 4. Social Engineering, Deepfakes, and DeepPhishing
- 5. Post-Engagement: Sharing Your Findings
- Summary & Takeaways

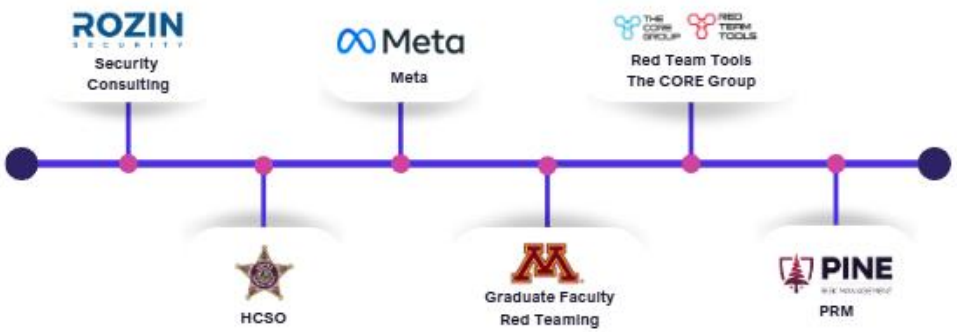
About Us

PRM: We conduct, build, and train red teams, helping organizations mature and improve security.
Meta: Started largest physical red team in Silicon Valley, hired dozens of testers, and built a team to oversee findings remediation across global office and data center footprint.

Ana



Shawn



RSAC 2025 Conference

Group Engagement

What is your experience with Physical Red Teaming?

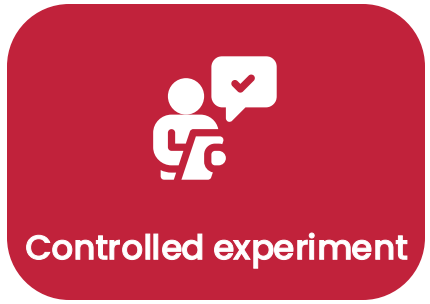
Many Voices.
One Community.

What is Red Teaming?

STRESS TESTING: TESTING THE SYSTEM WITH THE GOAL TO IMPROVE IT.

> The Red Team is the Blue Team in disguise.

RED TEAMING: BECAUSE HINDSIGHT IS TOO EXPENSIVE



PINE RISK MANAGEMENT

RSAC 2025 Conference

OUR ROLES

↘

The role of a red team is both:

- Security Scientist
- Sparring Partner

HOW DO WE KNOW SECURITY WORKS?

YOU TEST IT

Fail Safely: Testing your own security programs allows businesses to fail safely and uncover vulnerabilities before the bad guys do.

THEY TEST IT

Fail Catastrophically: Fail expensively. A real attack can be life-or-death for people, businesses, or systems.

RSAC 2025 Conference

Red Team Foundations

Similarities, Scoping, and De-Risking

Many Voices.
One Community.

Define Red Teaming

Stress Testing: Testing a system with the goal to improve it

Types of Red Teams

- Cybersecurity
- Physical Security
- AI
- Analytical Red Teaming
- Privacy

Define Red Teaming

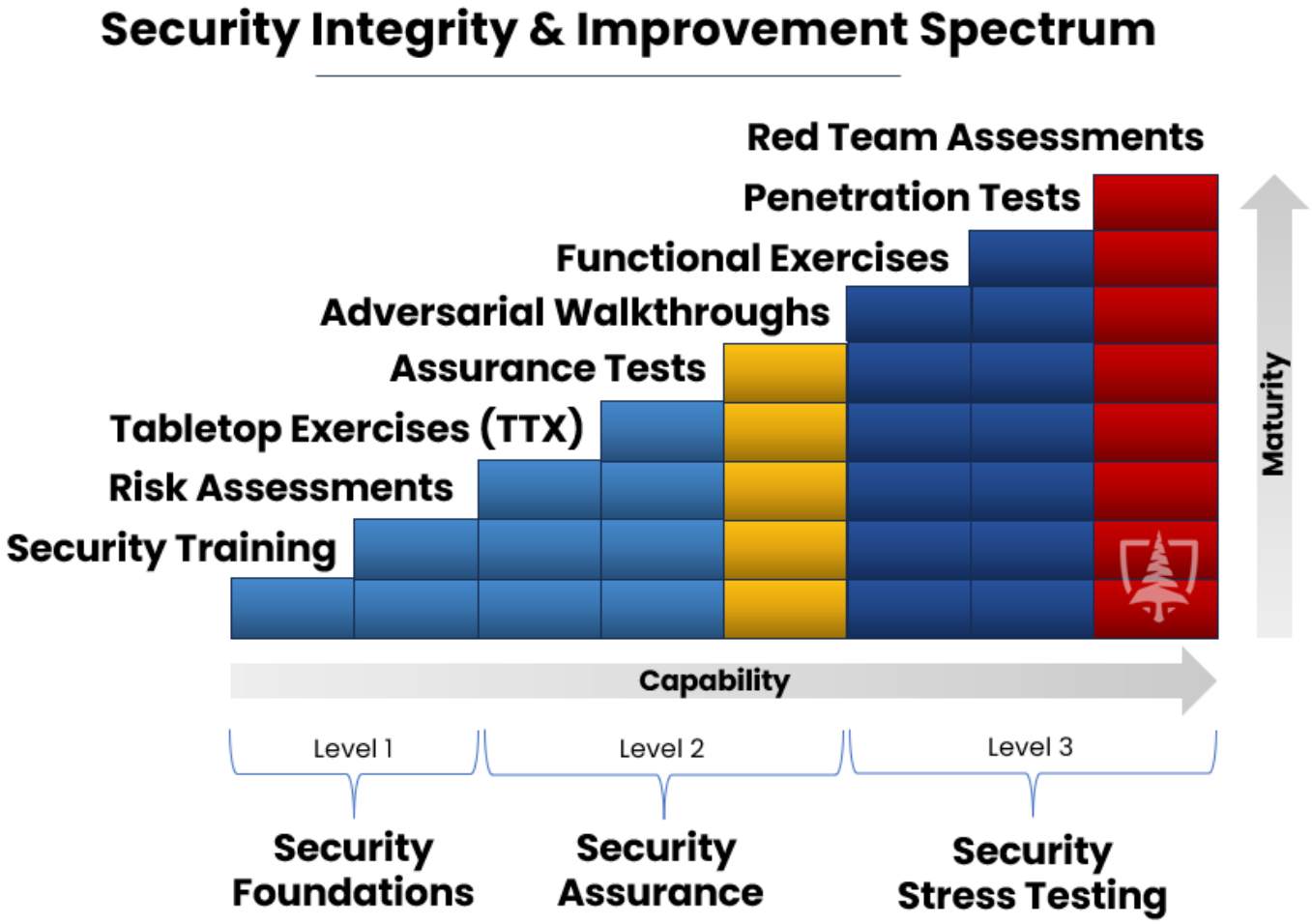
What type of assessment are you conducting?

The Red Team as a Blue Team in disguise.

Threat	**Focus:** Profiles probable attackers and their likely methods of attack. **Approach**: Identifies avenues of attack and the targeted hardware/software.	Start with WHO Then WHY, HOW, WHERE, and WHEN
Vulnerability	**Focus:** Identifies security vulnerabilities within the system. **Approach:** Quantifies the criticality of each vulnerability.	Test **Specific Controls** Focus on layers, locations, or control groups.
Asset	**Focus:** Identifies and prioritizes risks based on system assets. **Approach:** Evaluates the business impact of losing each asset.	Identify Assets Understand Consequences Steal the Assets

When is Red Teaming Right?

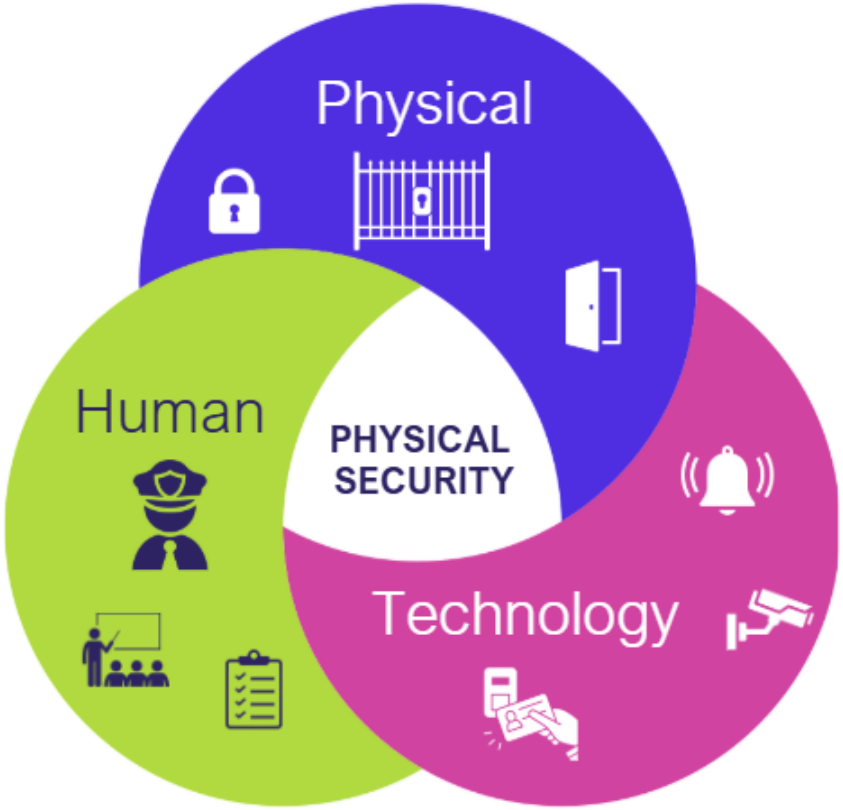
Crawl. Walk. Run.



© 2024 Pine Risk Management

Physical Security

Protecting People, Assets, and Reputation. Security measures that deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm.



Components of Physical Security

Physical: Doors, locks, gates, bollards, etc.

Technology: PACS, CCTV, Radios, Investigative, and Intelligence tools

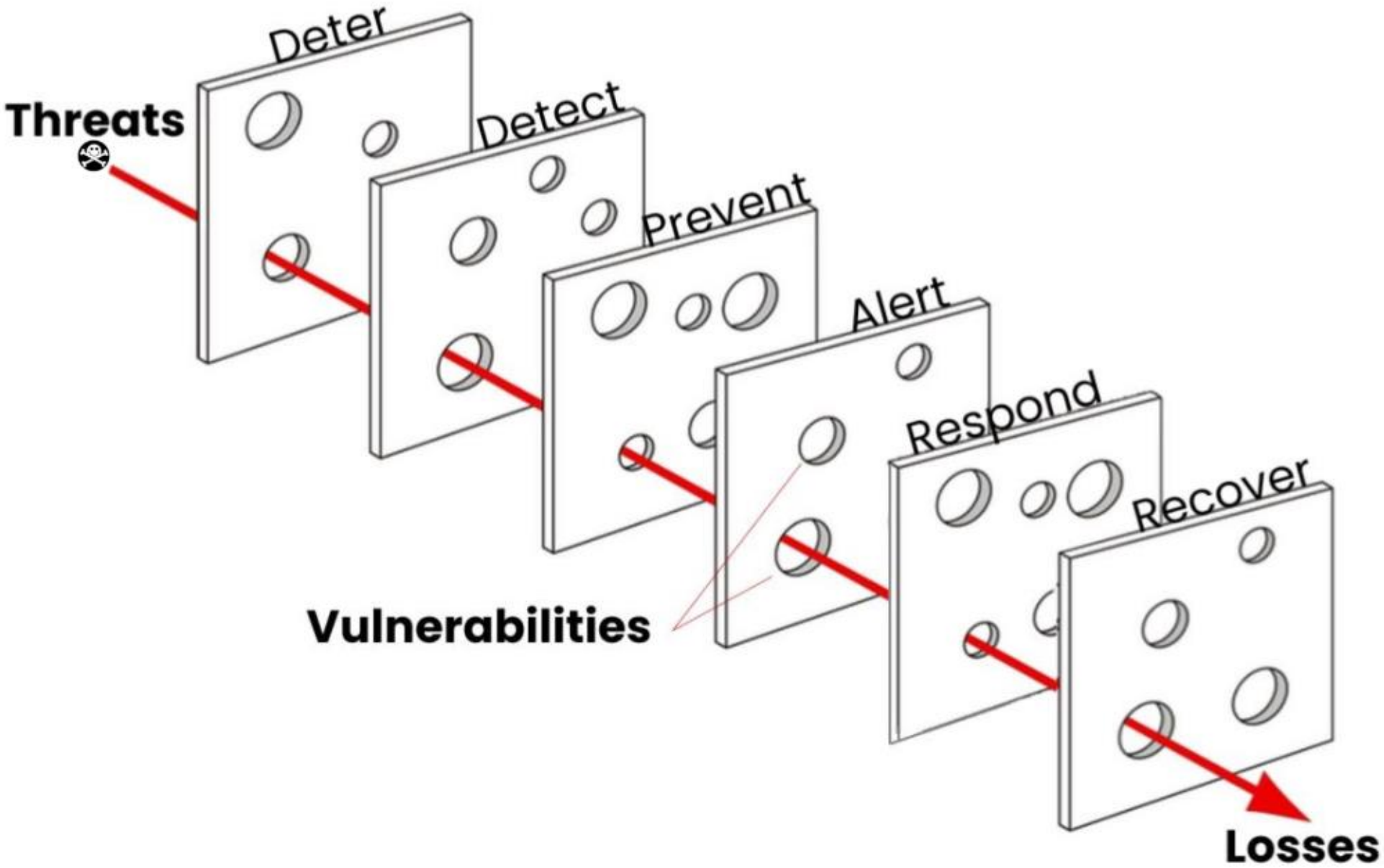
Human: Guards, Analysts, Managers, Awareness, Processes & Procedures

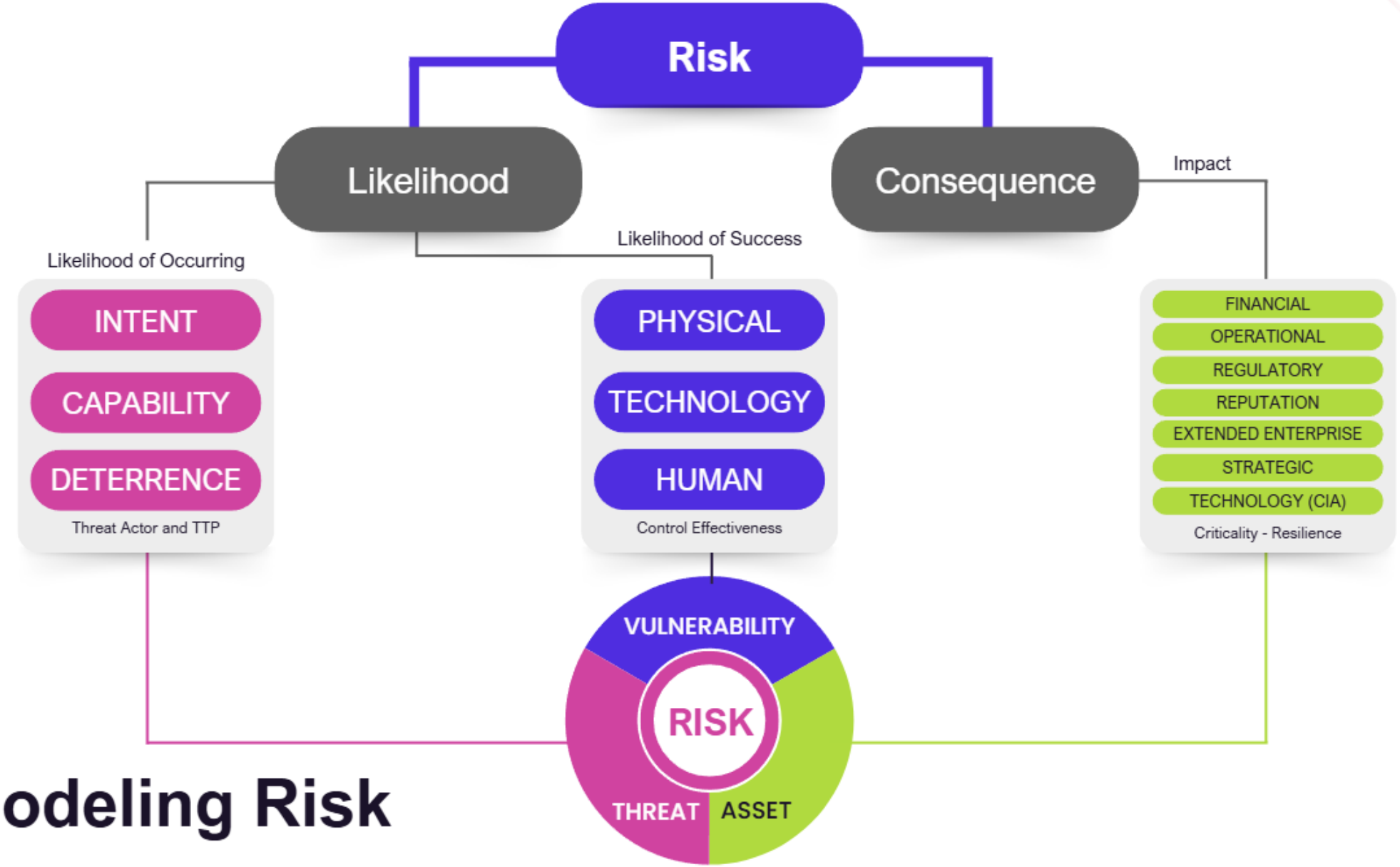
Physical Security

Physical Security Teams & Activities

Physical Security

Goals of Physical Security


Threats
Deter
Detect
Prevent
Alert
Respond
Recover
Vulnerabilities
Losses



Modeling Risk

RSAC 2025 Conference

Key Question

Have you done Threat Modeling for Physical scenarios?

Many Voices.
One Community.

Threat Modeling Ideation

Develop your threat model

A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment.

- **NIST 800-53**

Resource

Threat Modeling Overview

Basic Threat Modeling Visualization:

- Standard
- Long

Threat Modeling

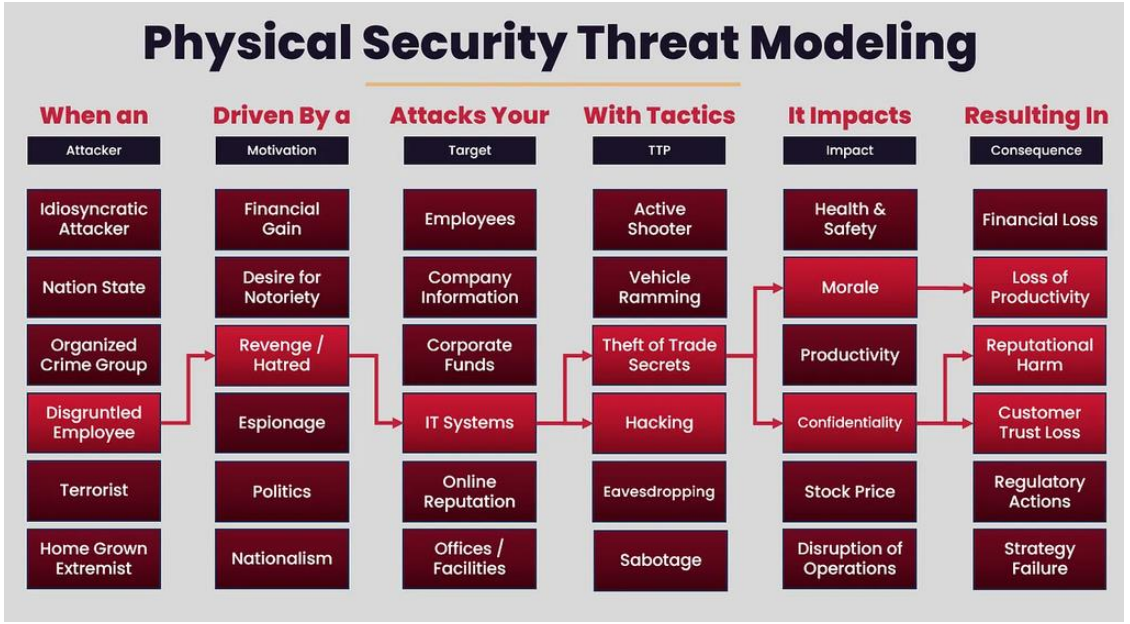
Mapping the Threat

Resource

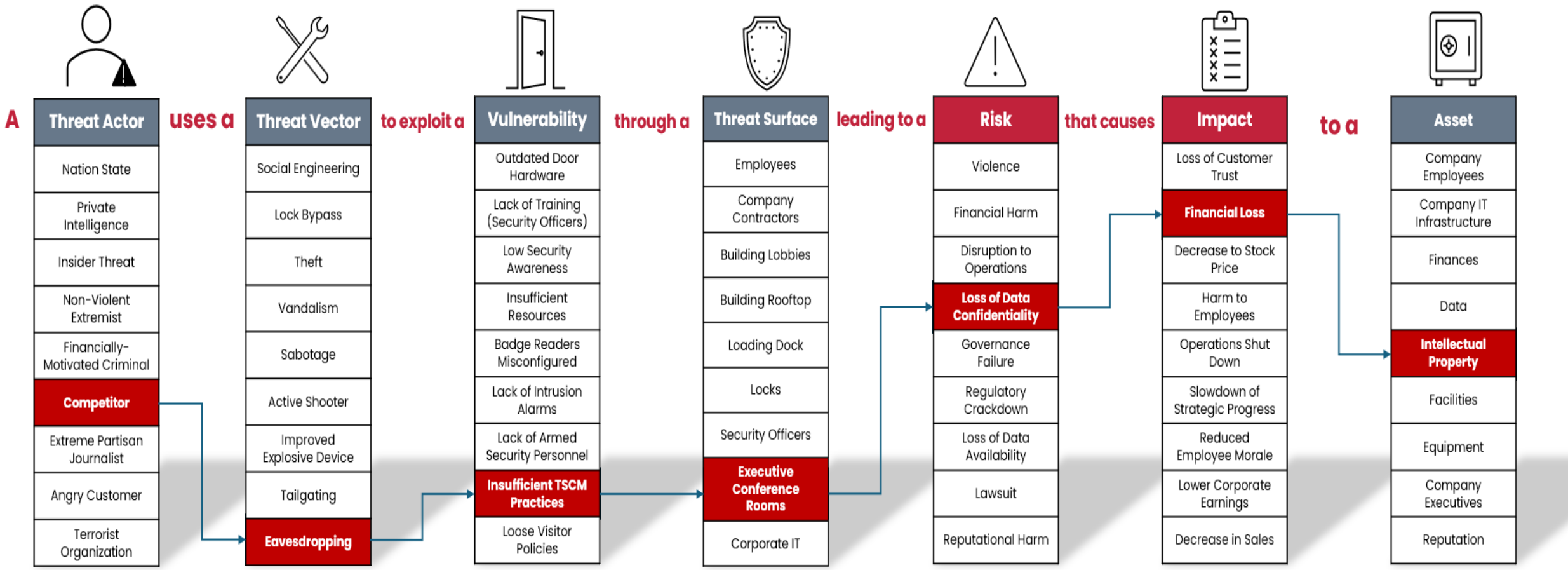
Physical Red Team Prioritization Matrix

Steps to Thread Modeling

1. Identify Assets
2. Define Adversaries
3. Define Attack Surface
4. List Attack Vectors
5. Identify Security Controls
6. Map Defenses to Threats
7. List Potential Vulnerabilities
8. Evaluate Likelihood & Impact
9. Prioritize Risks
10. Test Defenses and Countermeasures



Threat Modeling



RSAC 2025 Conference

Red Team Foundations: Similarities, Scoping, and De-Risking

Guidelines & Principles: Trust

Principles of Physical Red Teaming

Undercover

The Red Team is a Blue Team in Disguise

- Collaborate and support

Safe to Fail

Red Teaming is an Exercise

- Never fire people for failures
  Systemic, Not Individual
- Blameless Lessons Learned

Why

Do It for the Right Reasons

- No Ego

Be Creative

Think outside the box

- Test the untestable
- Don't limit yourself
- It's your role to think of things the blue team doesn't

Contribute to the Industry

Physical Security is relatively immature
Physical red teaming is even less mature as a profession

If you want to contribute:

Publish stories, write frameworks, give talks.

Develop tools, Open Source Them.

Learn about Physical Security: Go to a conference, take a course, and translate it to Cybersecurity professionals.

Take effective and mature aspects of the cybersecurity and try applying them to physical security.

Let's Get Physical

Seven Steps for Cyber Teams to Conduct Good Physical Assessments

Talk

Talk to the Physical Security Teams Early

Understand

Understand their needs, strengths, known weaknesses, goals, etc.

Scope

Focus on objectives

De-Risk

Get Authorization

Communicate

Before, during, and after with all necessary parties

Debrief

Show & Tell

Framing

Present, frame, and communicate your findings effectively. Know your audience. Technical terms don't work; pose it in terms of risk, threat model, and threat actors. They don't know what APTs are targeting your networks, so use the data you have to tell a compelling story.

RSAC 2025 Conference

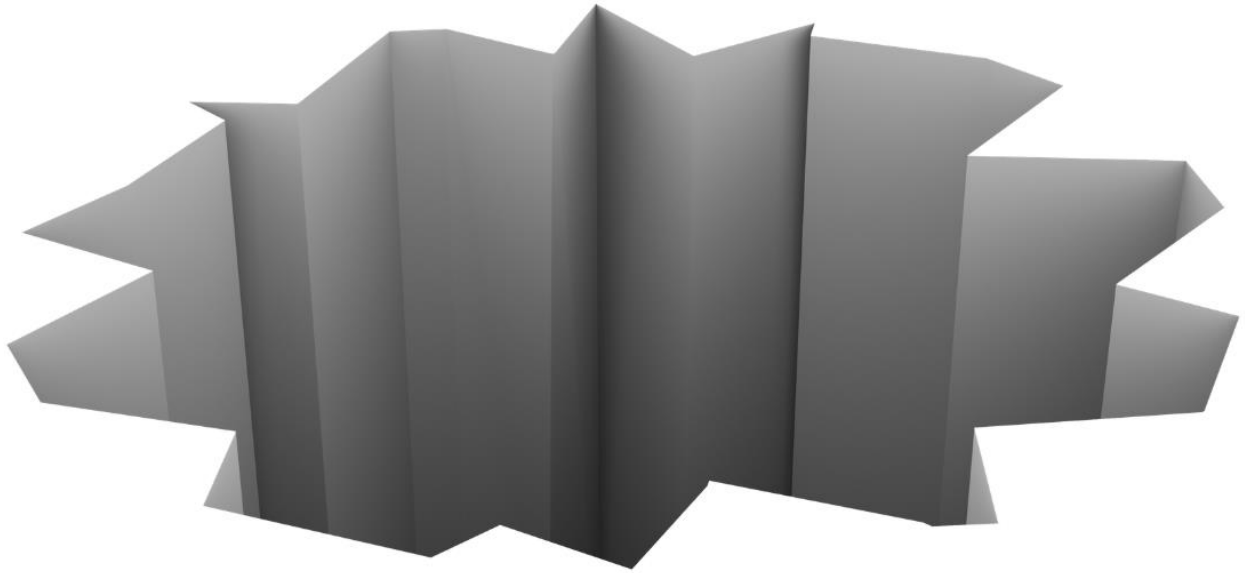
Red Team Foundations
Similarities, Scoping, and De-Risking

Common Pitfalls to Avoid

Common Pitfalls

DON'T:

- Cause or use uncomfortable social topics to gain entry (race, gender, etc.)
- Create more risk than you mitigate
- Bring your Politics to Red Teaming
- Commit Crimes (you're authorized, or not)
- Steamroll
- Brag (Afterward or outside of reporting chain)
- Do Cowboy Shit



The Don’t of Physical Red Teaming

DON’T:

- Create vulnerabilities and leave them (even if the client says it’s ok)Create more risk than you mitigate
- Break into the wrong floor
- Accidentally Assault Someone
- Reach for your LoA in your back pocket while a cop points an AR15 at you
- Get anyone fired
- Pay or take bribes

- Pay or take bribes

- Use a fake Letter of Authorization (Get out of Jail Free card)
- Make security’s job harder

RSAC 2025 Conference

Red Team Foundations
Similarities, Scoping, and De-Risking

Physical Assessments by Cybersecurity Professionals

Unique Risks of Physical Red Teaming Operators

Offensive Cybersecurity Team

Risk of Injury from
Attempted Access
Bystanders
Security
Law Enforcement

People respond Differently to burglary, theft, or assault than they do hacking

Lack of OpSec and physical VMs can lead to immediate arrest

Lack of knowledge, understanding, or expectation of physical penetration testing leads to escalations

Approach: Choose Your Player

Why are you testing physical security?

Physical Enabled Cyber

Full Physical Assessment

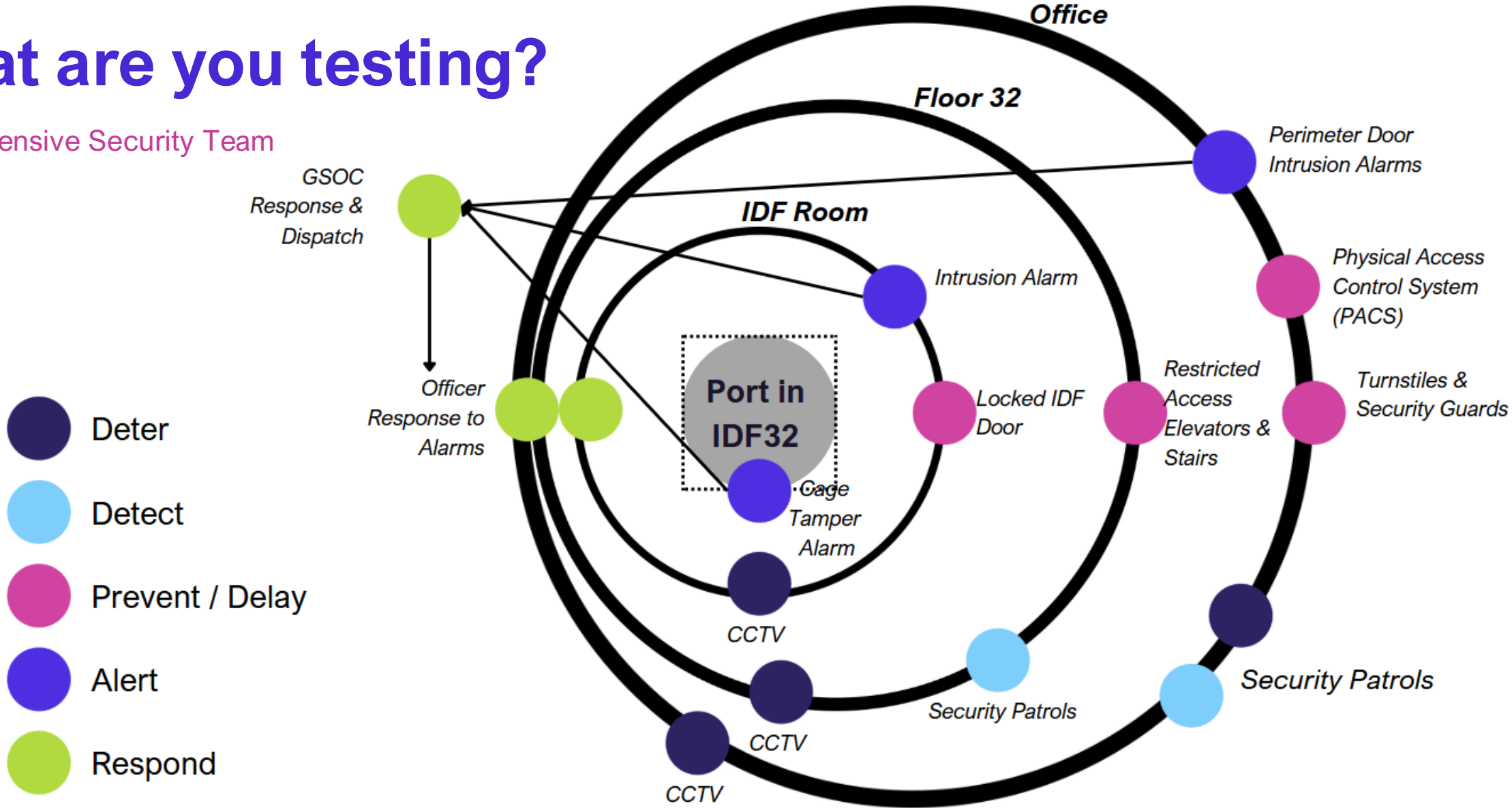
Cyber with a Twist

Test Specific Physical Controls

Test Physical Security Technology

What are you testing?

Offensive Security Team



Collaborating with PhySec

Offensive Cybersecurity Team

Threat Ideation:
Poison Circles

Physical-Enabled Cyber Vulnerability Sharing
Let them know your strengths and weaknesses.

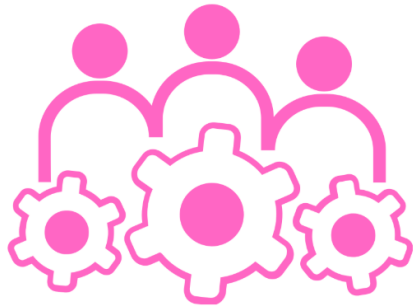
Access to office-area LAN
Access to server room
Access to racks in data center

Joint Operations:
Pull their folks into your assessment if you need a physical component

Inform Risk Assessments

Joint Training

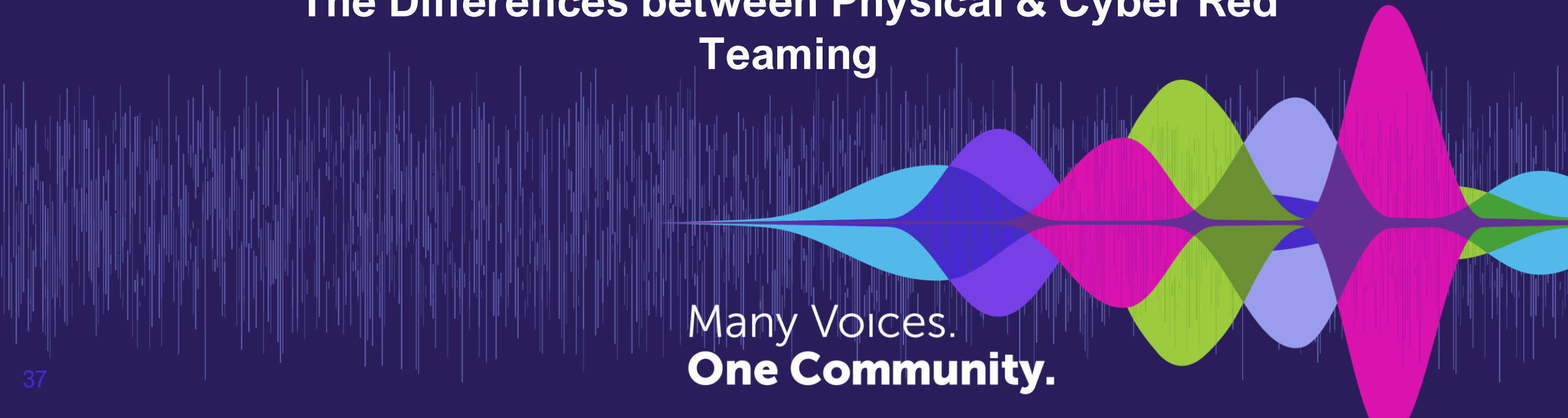
Overlap



RSAC 2025 Conference

Red Team Foundations
Similarities, Scoping, and De-Risking

The Differences between Physical & Cyber Red Teaming



Many Voices.
One Community.

Similarities in Testing

Approach – Adversary emulation / stress testing
Need for OpSec
Blue teamer in disguise
Kill-Chain

Security Objective	Prevent	Security Component	Human	Security Layer	Roof Access

Recon	Surveillance	Resource Development	Probing	Pretexting	Perimeter Breach	Facility Breach	Persistance	Priviledge Escalation	Defense Evasion	Discovery	Collection	Exfiltration	Impact
54 Techniques	17 Techniques	22 Techniques	44 Techniques	33 Techniques	37 Techniques	44 Techniques	52 Techniques	26 Techniques	32 Techniques	34 Techniques	46 Techniques	48 Techniques	54 Techniques
OSINT	Identify Security Measures	Impersonation	Testing physical barriers and locks	Posing as maintenance or repair personnel	Climbing fences or walls	Using stolen or counterfeit access cards	Creating hidden compartments within the facility	Using stolen or forged credentials	Disabling security cameras or alarms	Mapping out security camera locations	Gathering sensitive documents or data	Smuggling documents or data out of the facility	Destroying physical security systems or barriers
Linkedin Employee Search	Individual: Static Surveillance (sitting on bench or coffee shop nearby)	Purchase Clothing	Attempting to access restricted areas	Using fake identities to gain information	Cutting through barriers or fencing	Tailgating authorized personnel into buildings	Installing covert surveillance equipment	Exploiting software vulnerabilities	Using counterfeit identification	Identifying access control points	Recording audio or video of sensitive areas	Using encrypted communication channels	Tampering with critical infrastructure
Google Dorking	Individual: Dynamic Surveillance (walking around)	Print Lookalike Badges (BASED ON: OSINT of current employees)	Triggering alarms to observe response times	Pretending to be a new employee	Using vehicles to ram gates or barriers	Posing as cleaning or maintenance staff	Planting devices that can be remotely accessed	Manipulating access control systems	Erasing or manipulating logs	Surveying internal layout of the facility	Using covert cameras or recording devices	Transferring data to external storage devices	Disrupting power or communication lines
Recent News/Media	Vehicle-Based Surveillance		Conducting false maintenance requests	Creating fictitious scenarios to elicit information	Exploiting gaps or vealnesses in fencing	Forcing doors or windows open	Establishing redundant access points	Using social engineering to gain higher privileges	Disguising as authorized personnel	Gathering employee shift schedules	Collecting access credentials and badges	Sending data via email or file sharing services	Initiating fire or smoke to cause evacuations
Localized Image Search	Handheld Photography	Breach Tool Acquisition	Checking for unsecured doors or windows	Impersonating delivery or service workers	Using ladders or other tools to scale obstacles	Bypassing electronic access control systems	Using social engineering to maintain access	Installing backdoors or rootkits	Utilizing insider knowledge to avoid detection	Identifying key personnel and their routines	Harvesting information from unlocked computers	Using remote access tools for data transfer	Damaging key assets or equipment
	Covery Persistent Photography	Obtain specialized lockpicking tools based on site hardware (e.g., Knife, pick gun, tool bypass)	Using social engineering to gather access information	Posing as law enforcement or government officials	Digging tunnels or trenches to bypass barriers	Exploiting HVAC or utility access points	Hiding in seldom-used areas of the facility	Compromising administrator accounts	Using encryption to hide activities	Investigating security protocols and response times	Obtaining data from printers or copiers	Concealing data within other files or images	Compromising data integrity or availability
Obtain Facility Layout	Sensor Placement		Attempting to bypass security systems	Using social media profiles to gain trust	Disabling perimeter alarms or sensors	Using hidden compartments to smuggle tools	Setting up temporary camps or stations	Utilizing insider threats or collusion	Deploying decoys or distractions	Analyzing entry and exit logs	Collecting discarded documents from trash or recycling	Uploading data to cloud storage services	Introducing malware or ransomware
City construction permits		Bypass Tool Acquisition	Observing and testing security personnel reactions	Calling with urgent requests for information	Tailgating authorized personnel through gates	Deactivating alarm systems and sensors	Compromising janitorial or utility closets	Exploiting default passwords or settings	Avoiding security patrol routes	Searching for unmonitored or less-secured areas	Copying files from network shares or servers	Using physical drop points for data exchange	Manipulating environmental controls (e.g., HVAC)
City blueprints	Identify Vendors	Obtain shove-knife: under door tool, and other bypass tools.	Testing access control systems with fake credentials	Sending emails with fabricated stories	Using fake credentials to pass through checkpoints	Cloning access badges or keycards	Using false maintenance requests to stay onsite	Leveraging trust relationships between systems	Using stealth technology or techniques	Identifying locations of critical assets	Using USB drives or other portable storage devices	Sending data through secure tunnels or VPNs	Sabotaging network or IT infrastructure
Landlord rental site	Using drones to monitor the facility	Create mock-up of target site using surveillance and OSINT info											
	Monitoring employee and visitor patterns		Using social engineering to gather access information	Posing as law enforcement or government officials	Digging tunnels or trenches to bypass barriers	Exploiting HVAC or utility access points	Hiding in seldom-used areas of the facility	Compromising administrator accounts	Using encryption to hide activities	Investigating security protocols and response times	Obtaining data from printers or copiers	Concealing data within other files or images	Compromising data integrity or availability
Identify Vendors		Develop Cover Identity	Attempting to bypass security systems	Using social media profiles to gain trust	Disabling perimeter alarms or sensors	Using hidden compartments to smuggle tools	Setting up temporary camps or stations	Utilizing insider threats or collusion	Deploying decoys or distractions	Analyzing entry and exit logs	Collecting discarded documents from trash or recycling	Uploading data to cloud storage services	Introducing malware or ransomware
		Create website, email address, business cards, personas, and other cover documents											
Observation of site layout and security features	Continuous presence near entry and exit points	Acquiring tools and equipment for an operation	Testing physical barriers and locks	Posing as maintenance or repair personnel	Climbing fences or walls	Using stolen or counterfeit access cards	Creating hidden compartments within the facility	Using stolen or forged credentials	Disabling security cameras or alarms	Mapping out security camera locations	Gathering sensitive documents or data	Smuggling documents or data out of the facility	Destroying physical security systems or barriers
Questioning employees about site operations	Monitoring security personnel and routines	Renting or purchasing vehicles for surveillance	Attempting to access restricted areas	Using fake identities to gain information	Cutting through barriers or fencing	Tailgating authorized personnel into buildings	Installing covert surveillance equipment	Exploiting software vulnerabilities	Using counterfeit identification	Identifying access control points	Recording audio or video of sensitive areas	Using encrypted communication channels	Tampering with critical infrastructure
Noting security camera locations	Frequent observation of security cameras	Creating fake identification badges	Triggering alarms to observe response times	Pretending to be a new employee	Using vehicles to ram gates or barriers	Posing as cleaning or maintenance staff	Planting devices that can be remotely accessed	Manipulating access control systems	Erasing or manipulating logs	Surveying internal layout of the facility	Using covert cameras or recording devices	Transferring data to external storage devices	Disrupting power or communication lines
Recording entry and exit points	Taking photographs or videos of security features	Procuring uniforms that resemble security staff	Conducting false maintenance requests	Creating fictitious scenarios to elicit information	Exploiting gaps or vealnesses in fencing	Forcing doors or windows open	Establishing redundant access points	Using social engineering to gain higher privileges	Disguising as authorized personnel	Gathering employee shift schedules	Collecting access credentials and badges	Sending data via email or file sharing services	Initiating fire or smoke to cause evacuations
Mapping out patrol routes	Using binoculars or long-range cameras	Setting up safe houses or staging areas	Checking for unsecured doors or windows	Impersonating delivery or service workers	Using ladders or other tools to scale obstacles	Bypassing electronic access control systems	Using social engineering to maintain access	Installing backdoors or rootkits	Utilizing insider knowledge to avoid detection	Identifying key personnel and their routines	Harvesting information from unlocked computers	Using remote access tools for data transfer	Damaging key assets or equipment
Observing shift changes and employee routines	Setting up hidden cameras or recording devices	Obtaining maps and blueprints of the facility	Using social engineering to gather access information	Posing as law enforcement or government officials	Digging tunnels or trenches to bypass barriers	Exploiting HVAC or utility access points	Hiding in seldom-used areas of the facility	Compromising administrator accounts	Using encryption to hide activities	Investigating security protocols and response times	Obtaining data from printers or copiers	Concealing data within other files or images	Compromising data integrity or availability
Identifying blind spots in surveillance coverage	Conducting foot or vehicle patrols around the site	Securing communication devices and channels	Attempting to bypass security systems	Using social media profiles to gain trust	Disabling perimeter alarms or sensors	Using hidden compartments to smuggle tools	Setting up temporary camps or stations	Utilizing insider threats or collusion	Deploying decoys or distractions	Analyzing entry and exit logs	Collecting discarded documents from trash or recycling	Uploading data to cloud storage services	Introducing malware or ransomware
Analyzing building schematics or blueprints	Using drones to monitor the facility	Developing escape routes and contingency plans	Observing and testing security personnel reactions	Calling with urgent requests for information	Tailgating authorized personnel through gates	Deactivating alarm systems and sensors	Compromising janitorial or utility closets	Exploiting default passwords or settings	Avoiding security patrol routes	Searching for unmonitored or less-secured areas	Copying files from network shares or servers	Using physical drop points for data exchange	Manipulating environmental controls (e.g., HVAC)
Using drones for aerial surveillance	Monitoring employee and visitor patterns	Gathering financial resources for bribes	Testing access control systems with fake credentials	Sending emails with fabricated stories	Using fake credentials to pass through checkpoints	Cloning access badges or keycards	Using false maintenance requests to stay onsite	Leveraging trust relationships between systems	Using stealth technology or techniques	Identifying locations of critical assets	Using USB drives or other portable storage devices	Sending data through secure tunnels or VPNs	Sabotaging network or IT infrastructure
Monitoring delivery and service schedules	Following security personnel to and from the site	Assembling a team with specialized skills	Probing network or electronic security systems	Pretending to be a client or customer	Sneaking through service or delivery entrances	Breaking through less-secured entry points	Developing relationships with staff to avoid suspicion	Gaining physical access to restricted devices	Covering or altering physical appearance	Scanning for wireless networks and devices	Collecting information from public displays	Utilizing disposable or burner devices	Causing physical harm to personnel
Checking for public Wi-Fi networks	Using GPS trackers on vehicles	Acquiring surveillance equipment	Placing objects to test security attention	Using fake credentials or badges	Exploiting maintenance or construction areas	Utilizing service elevators or back stairways	Rotating personnel to avoid detection	Planting malicious hardware or software	Disabling or tampering with security devices	Conducting dumpster diving for discarded documents	Harvesting data from mobile devices	Transferring data over compromised network connections	Disabling alarm systems or sensors
Social engineering attempts to gather information	Listening to radio or communications traffic	Setting up decoy companies or personas	Using decoy packages to test mailroom procedures	Posing as contractors or consultants	Using drones to deliver payloads over barriers	Exploiting security desk or guard post distractions	Establishing sleeper cells or long-term presence	Exploiting gaps in security policies	Utilizing dark web or black market resources	Using social engineering to gather insider information	Recording keystrokes or screen captures	Using mobile devices for data exfiltration	Triggering false alarms to cause confusion
Identifying security weaknesses through social media	Analyzing guard shift changes	Stockpiling supplies like food and water	Attempting to access sensitive areas without authorization	Creating elaborate backstories for credibility	Employing decoys to distract security personnel	Using insider assistance to gain access	Utilizing fake identities to regularly re-enter	Utilizing phishing attacks to gain credentials	Hiding in blind spots or unmonitored areas	Surveying for hidden or covert security measures	Copying access logs or security records	Sending data through hidden network channels	Vandalizing property or defacing surfaces
Watching for security drills and responses	Observing and noting down security response times	Securing transportation routes and methods	Conducting false deliveries to gain entry	Impersonating vendors or suppliers	Posing as delivery or service personnel	Disguising as high-authority personnel	Placing long-term listening devices	Compromising multi-factor authentication methods	Using false credentials to avoid suspicion	Mapping out internal and external patrol routes	Collecting emails or internal communications	Concealing data within legitimate traffic	Stealing critical assets or information
Taking photographs of critical infrastructure	Pretending to be maintenance or delivery personnel	Building custom tools for bypassing security	Observing the response to minor security breaches	Pretending to be part of the IT or security team	Timing breaches during shift changes or low activity	Using forged documents or work orders	Using compromised IT systems for continued access	Hijacking user sessions	Altering or forging documents	Identifying maintenance and service schedules	Gathering data from backup or archival systems	Using steganography to hide data	Disrupting business operations
Using binoculars or long-range cameras	Mapping out the location of all security posts	Creating fake social media profiles for credibility	Placing suspicious items to test detection	Using fake documents to support identity claims	Utilizing natural cover (e.g., trees, bushes) to hide movements	Timing breaches during peak activity or shift changes	Employing hidden cameras or recording devices	Exploiting privilege escalation vulnerabilities	Creating fake emergency situations	Investigating physical and electronic security layers	Taking photographs of sensitive documents or screens	Physically removing hard drives or storage media	Manipulating safety systems (e.g., fire suppression)
Observing access control procedures	Using social media to track security schedules	Learning about security systems and technologies	Creating diversions to distract security	Calling from spoofed numbers to gain information	Creating diversions to draw security away	Placing tampered security devices to bypass checks	Manipulating security systems to avoid detection	Using brute force attacks on administrative accounts	Manipulating environmental controls (e.g., lighting)	Mapping network and communication infrastructure	Using network sniffing tools to capture data	Mailing physical copies of sensitive information	Contaminating water or air supply
Monitoring security checkpoints	Installing keyloggers on public computers	Developing cyber tools for hybrid attacks	Testing the effectiveness of surveillance cameras	Sending fake invoices or purchase orders	Exploiting unmonitored areas of the perimeter	Exploiting gaps in surveillance camera coverage	Creating backdoor access through software or hardware	Bypassing access control mechanisms	Avoiding detection by timing activities carefully	Identifying weaknesses in emergency procedures	Collecting data from fax machines	Using trusted insiders for data transfer	Causing financial loss through theft or damage
Surveying parking lot usage	Placing decoy items to observe response actions	Acquiring information through black market sources	Checking for unmonitored entry points	Using pretexts to conduct surveillance	Using grappling hooks or ropes	Using thermal or infrared devices to navigate in the dark	Utilizing abandoned or infrequently used rooms	Compromising network infrastructure	Using secure communication channels	Analyzing public records for building schematics	Harvesting data from cloud services	Exfiltrating data during shift changes or off-hours	Compromising backup or recovery systems

RSAC 2025 Conference

Physical TTPs
Tools of the Trade

Vulnerability Severity

Tier 5:
Advanced Nation-States
& Researchers

Tier 3:
Restricted Knowledge
Organized Crime / Insiders

Tier 1:
Any Teenager
with YouTube

Tier 4:
Government Circles
Private Brokers

Tier 2:
Some specialized
knowledge & skill

Wiegand Interception

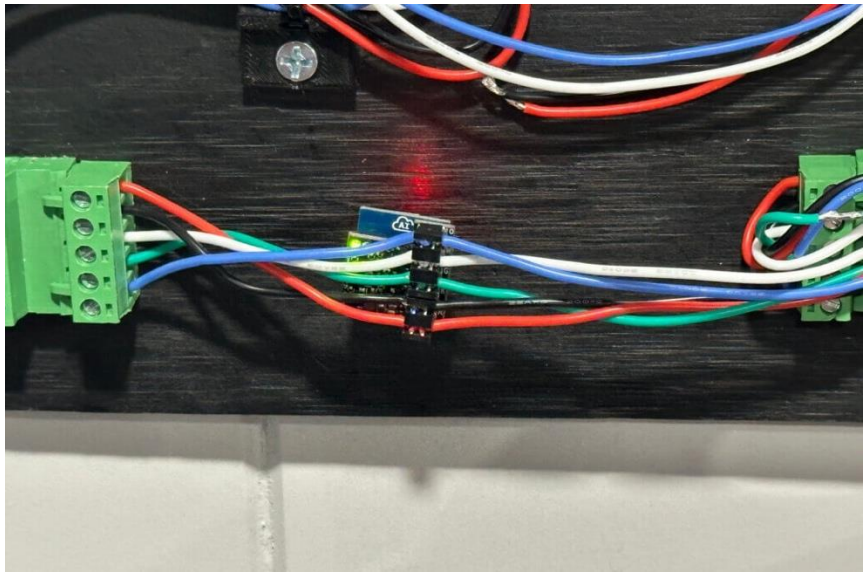
ESPKey Tool

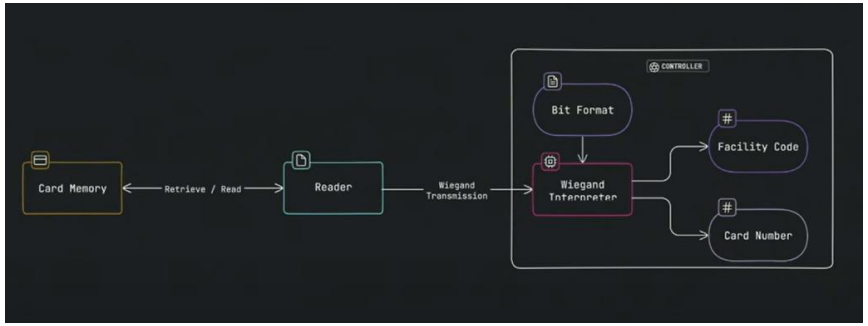
User's Guide

ESPKey
Wiegand Interception Tool
By Octosavvi

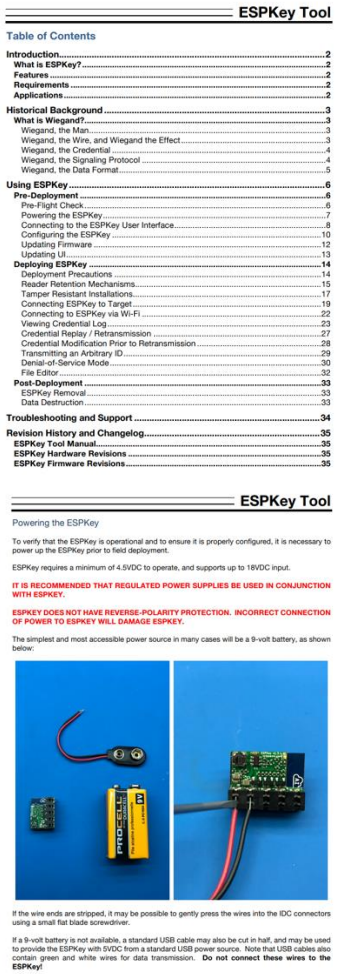
Current Revision
Document v1.0.0
Hardware v1.3.1
Firmware v128

The latest version of this document may be obtained from Red Team Tools:
http://www.redteamtools.com/espkey





Source: High Intensity Destruction (DC32 Talk) & RedTeamTools.com



ESPKey Tool

Table of Contents

Introduction....2
What is ESPKey?....2
Features....2
Requirements....2
Applications....2
Historical Background....3
What is Wiegand?....3
Wiegand, the Man....3
Wiegand, the Wire, and Wiegand the Effect....3
Wiegand, the Credential....4
Wiegand, the Signaling Protocol....4
Wiegand, the Data Format....5
Using ESPKey....6
Pre-Deployment....6
Pre-Flight Check....6
Powering the ESPKey....7
Connecting to the ESPKey User Interface....8
Configuring the ESPKey....10
Updating Firmware....12
Updating UI....13
Deploying ESPKey....14
Deployment Precautions....14
Reader Retention Mechanisms....15
Tamper Resistant Installations....17
Connecting ESPKey to Target....19
Connecting to ESPKey via Wi-Fi....22
Viewing Credential Log....23
Credential Replay / Retransmission....27
Credential Modification Prior to Retransmission....28
Transmitting an Arbitrary ID....29
Denial-of-Service Mode....30
File Editor....32
Post-Deployment....33
ESPKey Removal....33
Data Destruction....33
Troubleshooting and Support....34
Revision History and Changelog....35
ESPKey Tool Manual....35
ESPKey Hardware Revisions....35
ESPKey Firmware Revisions....35

ESPKey Tool

Powering the ESPKey

To verify that the ESPKey is operational and to ensure it is properly configured, it is necessary to power up the ESPKey prior to field deployment.

ESPKey requires a minimum of 4.5VDC to operate, and supports up to 18VDC input.

IT IS RECOMMENDED THAT REGULATED POWER SUPPLIES BE USED IN CONJUNCTION WITH ESPKEY.

ESPKEY DOES NOT HAVE REVERSE-POLARITY PROTECTION. INCORRECT CONNECTION OF POWER TO ESPKEY WILL DAMAGE ESPKEY.

The simplest and most accessible power source in many cases will be a 9-volt battery, as shown below:

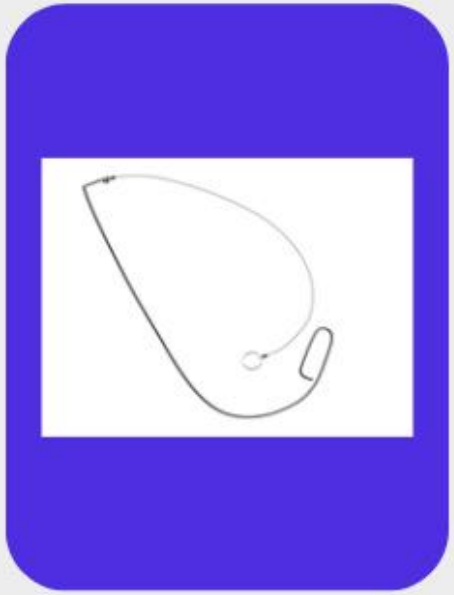
If the wire ends are stripped, it may be possible to gently press the wires into the IDC connectors using a small flat blade screwdriver.

If a 9-volt battery is not available, a standard USB cable may also be cut in half, and may be used to provide the ESPKey with 5VDC from a standard USB power source. Note that USB cables also contain green and white wires for data transmission. **Do not connect these wires to the ESPKey!**

PINE RISK MANAGEMENT

The Four Horsemen of PRT

Under Door Tool

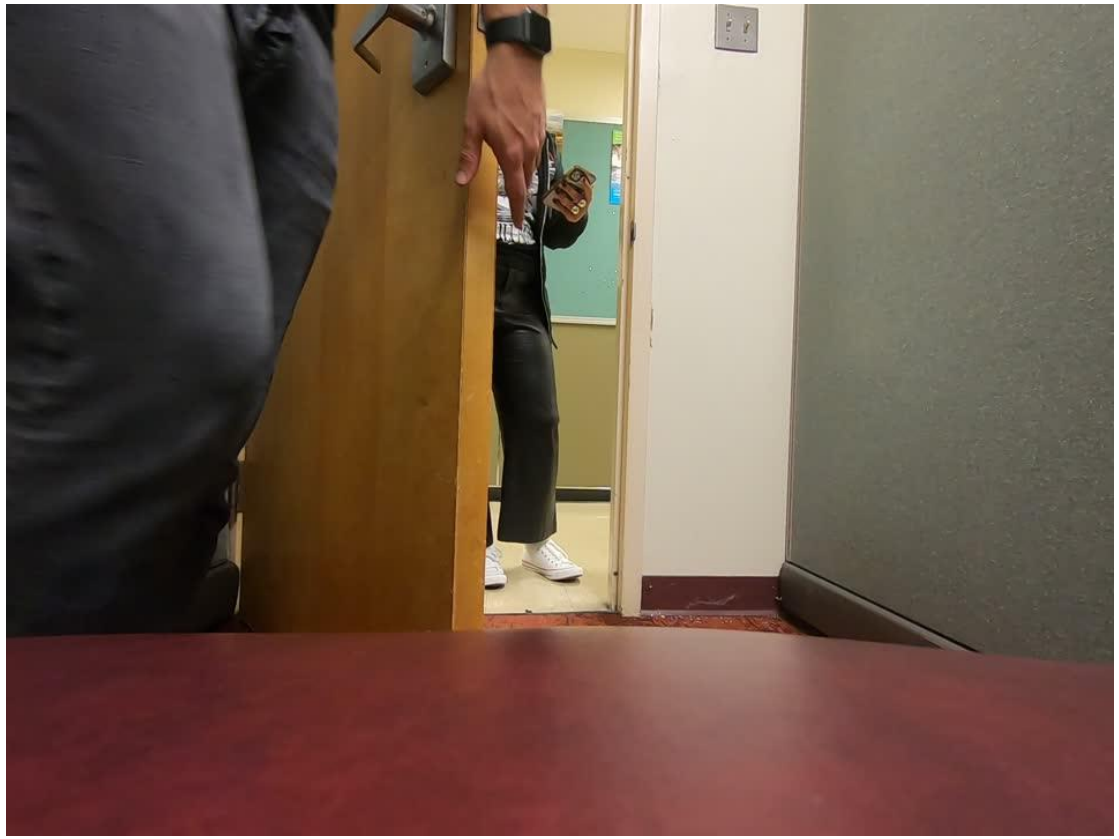


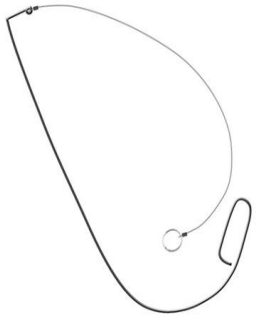
Canned Air

Latch Jim / Shove-It

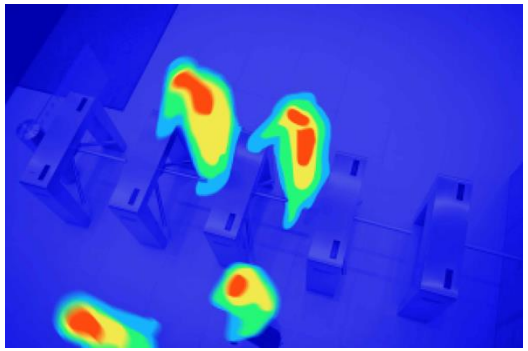
ESPKey

Under Door Tool

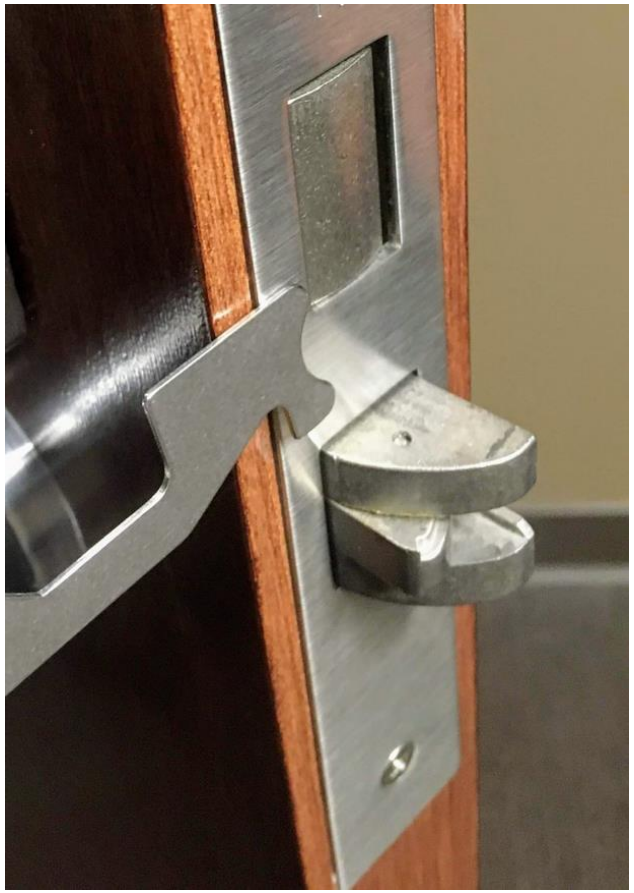




Canned Air & Rex Sensors

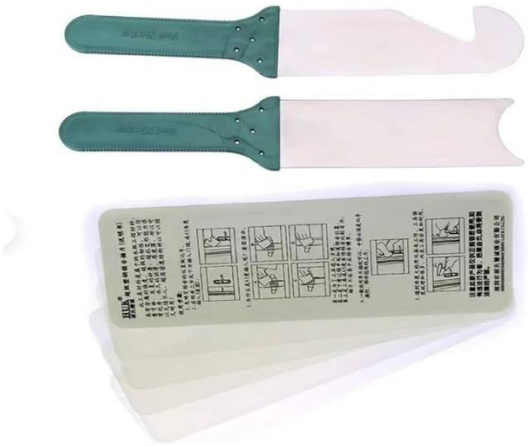


Shove Knife / Rescue Jim

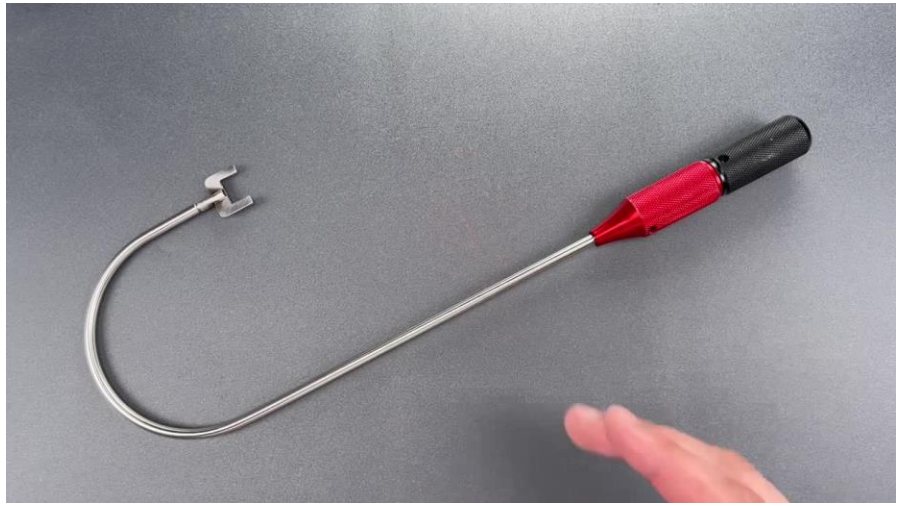


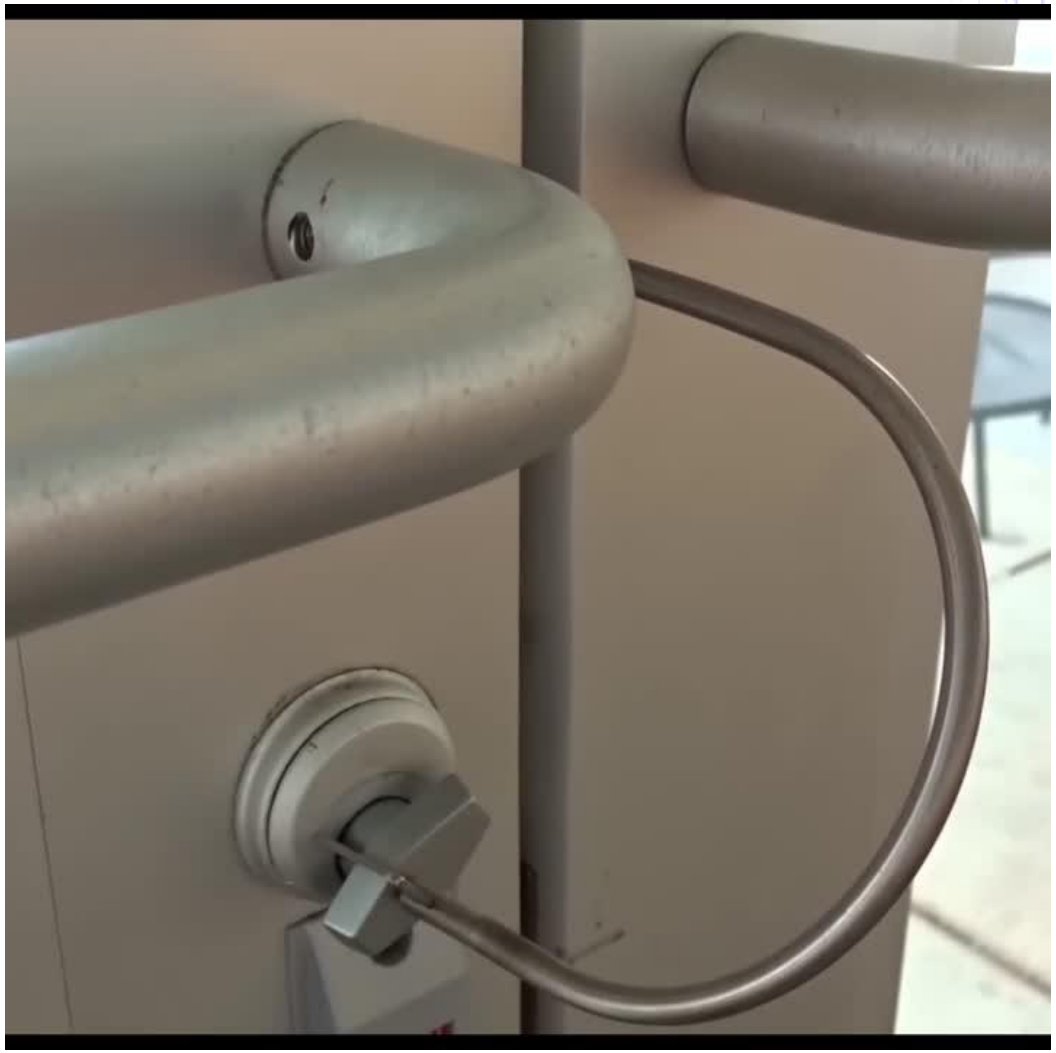
ESPKeys & Weigand Interception

Door Shims



Commercial Door Hooks & J Tool





Key-Pain

T-Pain
@TPAIN

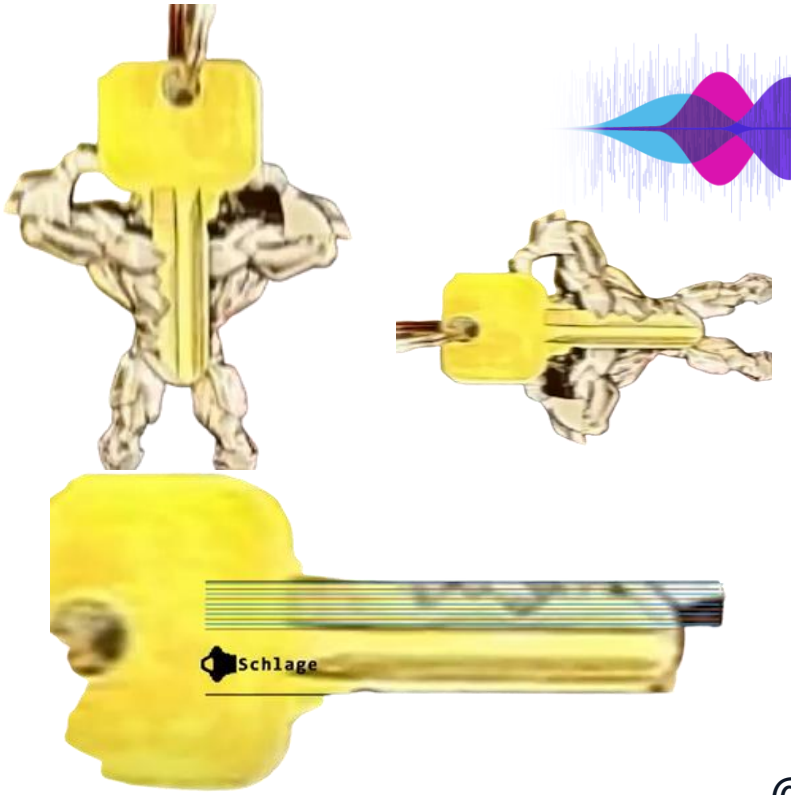
I DID IT BOIS!!!! Im officially a restaurant owner. Got my keys today and I'm scared as shit. BUT! I can no longer ignore the paths God has set for me just because I don't understand or I'm scared. (1/4)

T-Pain
@TPAIN

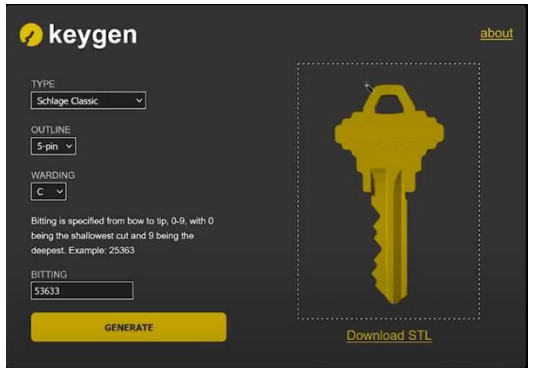
Replying to @TeosGirlfriend6

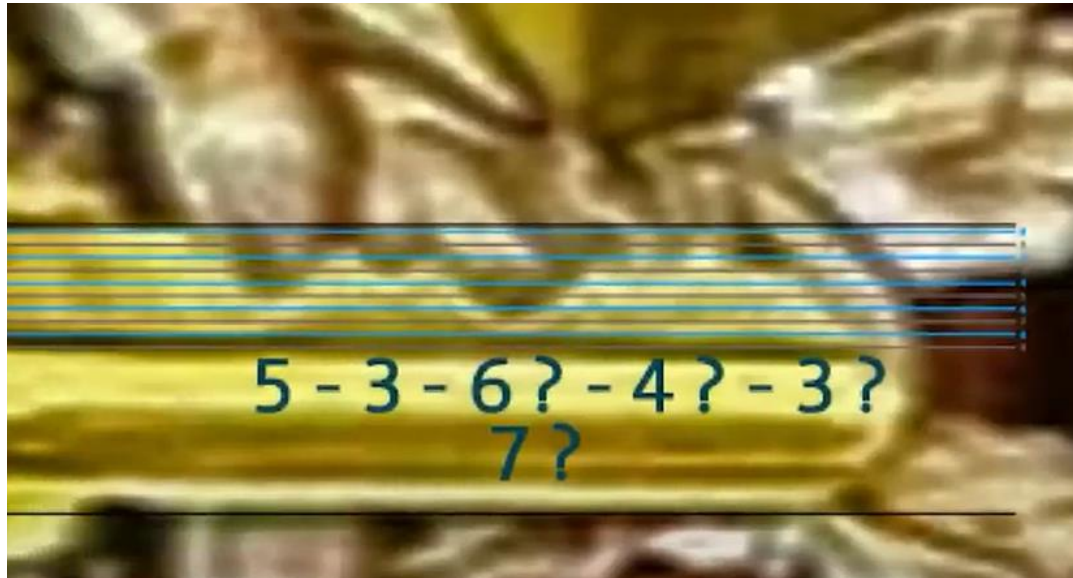
Then what? You gonna take some cups and a chair? 😂 Thanks for the heads up tho. I just got the keys today. No way the locks are gonna be the same next week. Thanx tho

9:06 PM · May 8, 2022 · Twitterrific for iOS



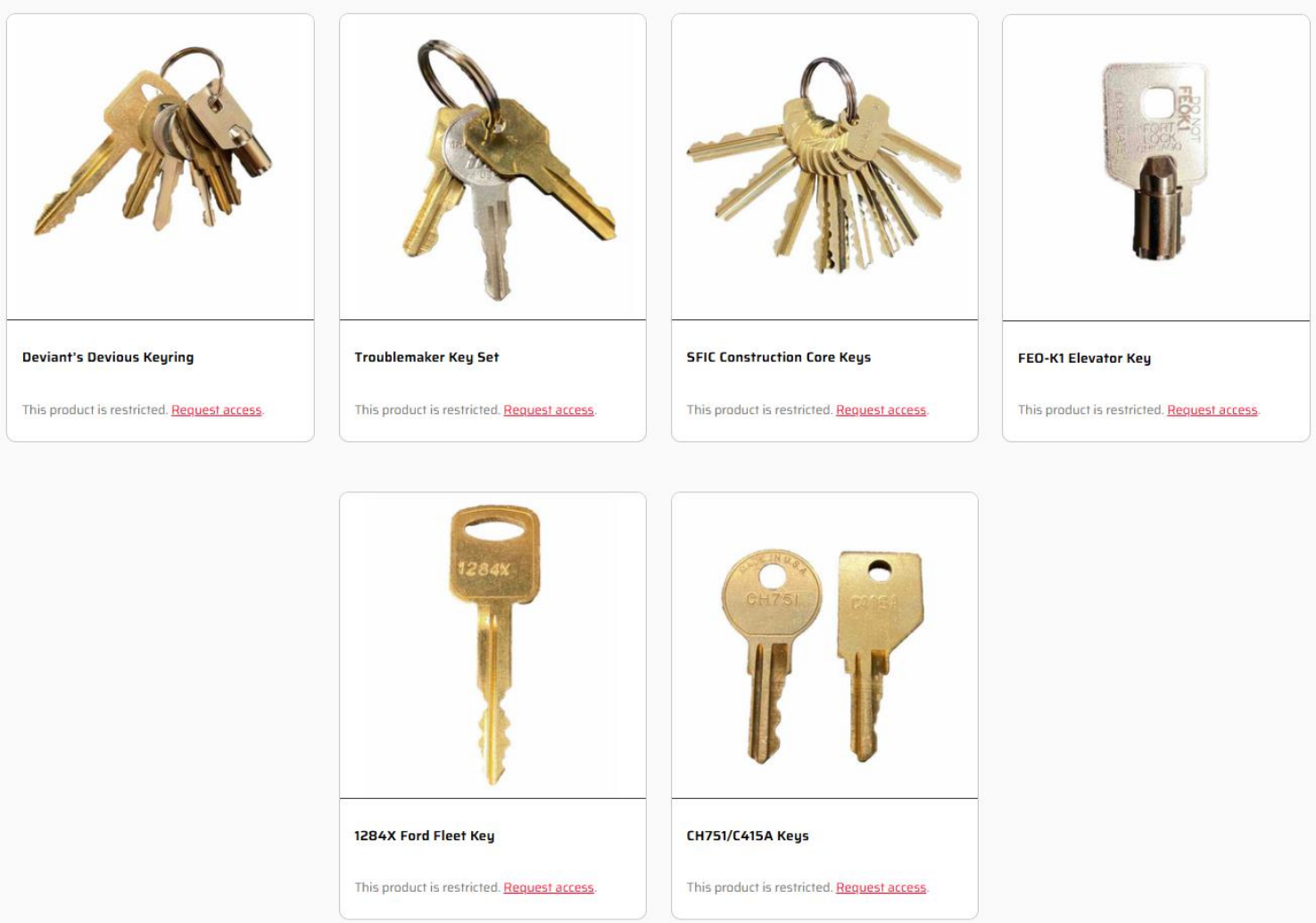
Source:
@DeviantOllam





PINE
RISK MANAGEMENT

Common Keys



Deviant's Devious Keyring

This product is restricted. Request access.

Troublemaker Key Set

This product is restricted. Request access.

SFIC Construction Core Keys

This product is restricted. Request access.

FEO-K1 Elevator Key

This product is restricted. Request access.

1284X Ford Fleet Key

This product is restricted. Request access.

CH751/C415A Keys

This product is restricted. Request access.

New Tools: WMD & LRR

Surveillance

Surveillance

Social Engineering

What is Social Engineering?

NIST 800-115:

- *"The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust."*

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Types of SE

- In Person
- Phishing
- Vishing
- Smishing
- Deep Fakes / Deep Vishing

Social Engineering

Tips & Tricks for Successful SE Attacks

The Best Lie

is

Closest to the Truth

Detection Apprehension
Cognitive Load

Social Engineering

Tips & Tricks for Successful SE Attacks

Mirroring

Body Language

Feet Direction

Voice

Volume

Tone

Social Engineering

Tips & Tricks for Successful SE Attacks

Disguises

Avoid Overkill (Movies)

Bright Colors

Voice & Body Language

Enable Surveillance

Enable Access

Social Engineering

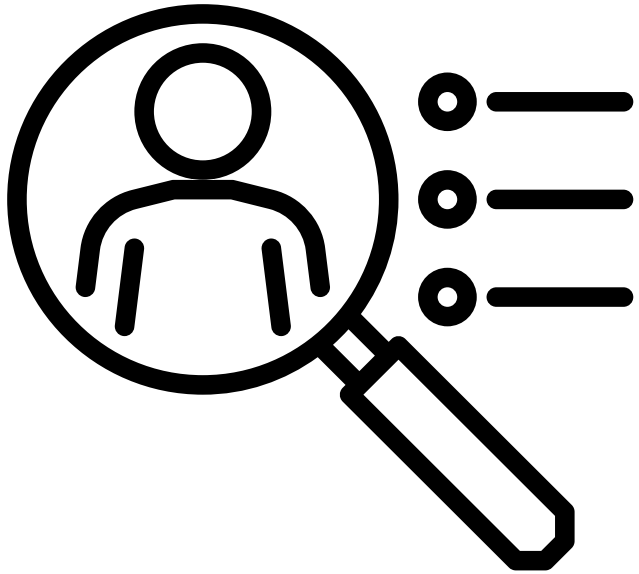
Tips & Tricks for Successful SE Attacks

Contextual Profile

Belongings
Body Language
Walking Speed
Eye Contact
Demeanor

Social Engineering

Tips & Tricks for Successful SE Attacks



Scenario Building

Research

Build Scenarios

Create Similarities

Have an Out

Social Engineering

Tips & Tricks for Successful SE Attacks

Authority Borrowing

Dress & Demeanor

Vocabulary

Props

Confidence

Social Engineering

Tips & Tricks for Successful SE Attacks

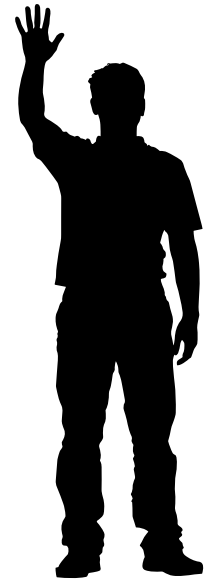
First to Greet Wins

Initiate Contact

Display Comfort

Act Like You Belong

Be the Assumed Insider



Social Engineering

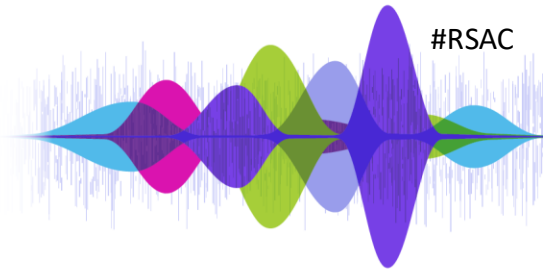
Tips & Tricks for Successful SE Attacks

Silence is Golden

Create Gentle Discomfort

Let them Assume You're Legit

Silence Leds to Yes



Probing Security

Testing your Hypotheses

Goals of Probing

- Gather information that requires active measures (recon is passive)
- Assess security's response to various scenarios
- Opportunistic: Low-risk probing may reveal opportunities to enter
  Decide if you're ready to execute the assessment
- Test hypotheses that your breach attempts rely on
- May be combined with recon

RSAC 2025 Conference

Physical TTPs Tools of the Trade

GenAI in Offensive Security

Many Voices.
One Community.

AI Surveillance: Lip Reading

Yeah but these numbers go out in two days and tear way stronger than our queue for numbers last year. Plus we're not mentioning the merger yet, that will send shutter price through the roof

No...no

We have to add that to the shareholder call. If we don't and the regulators find out, they'll be all up in your business and legal says they're likely to finance if we're not fully transparent

Ethics Questions

Doing the Right Thing

Scenario

- **Goal:** Break into a high-security building
- **Test:** One security officer provides job and schedule info, one escorts you inside to find a lost wallet, and one offers you access to the executive space in exchange for a fake COVID-19 vaccination card (required or they get fired).
- **Question:** How do you report these incidents? When? Do you include names?

Don't Get People Fired... Except in Extreme cases

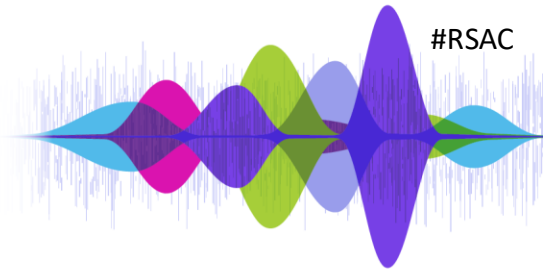
Naming Leads to Scapegoating

Bribes get tricky very quickly

Blue Team in Disguise
Always do a root cause

RSAC 2025 Conference

Group Engagement



AI for Physical Pen Testing

- **Phishing**: Improved scenarios, automated interactions, and automated Spearphishing
- **Voice Cloning**: Recording or live
- **DeepVishing**: Calls or Video with cloned faces and voices
- **MassVishing**: Targeting an entire organization with realistic automated bots
- **Automated Distractions**: “I’m stuck in the stairwell”
- **Lip Reading**: Long-distance video
- **GeoInt**: Automatically identify locations, technologies, and vulnerabilities.

Group Exercises & Demos

Team 1: Enablement

- Prioritization
- Threat Modeling
- Planning

Team 2: Pre-Operational Activity

- OSINT
- Surveillance & Recon

Team 3: Execution

- Practice your TTPs

PineRisk.com/RSAC

RSAC 2025 Conference

Bringing It All Together

Target Acquired:
How to Make a Difference Following an Assessment

Many Voices.
One Community.

Ten Steps for Physical Red Teaming

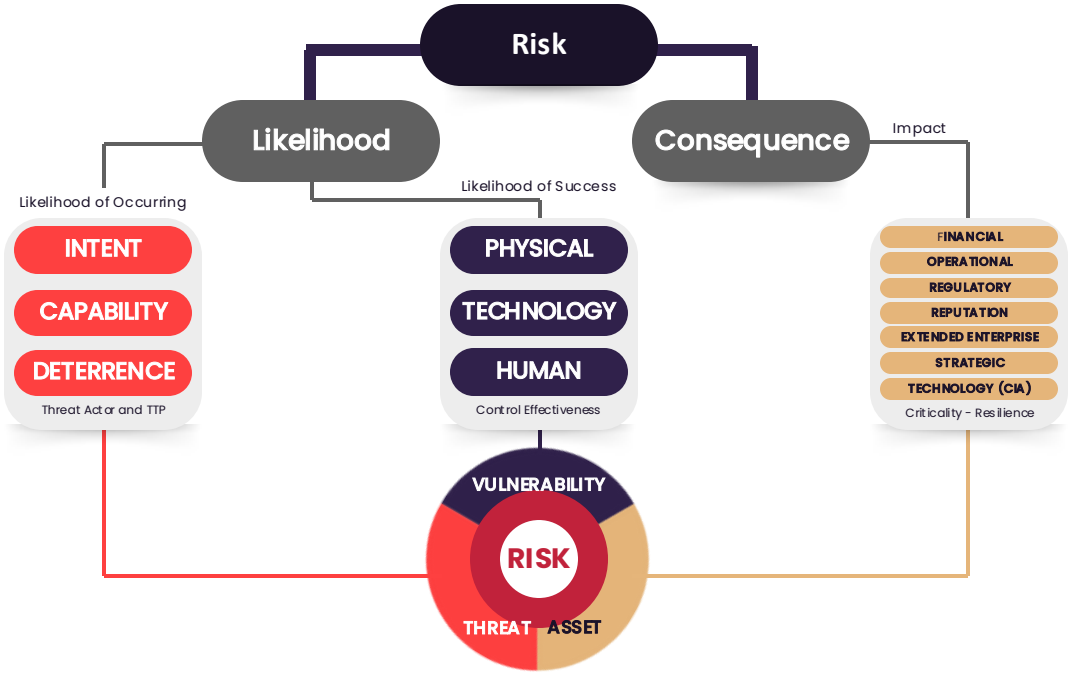
Running a Red Team Operation

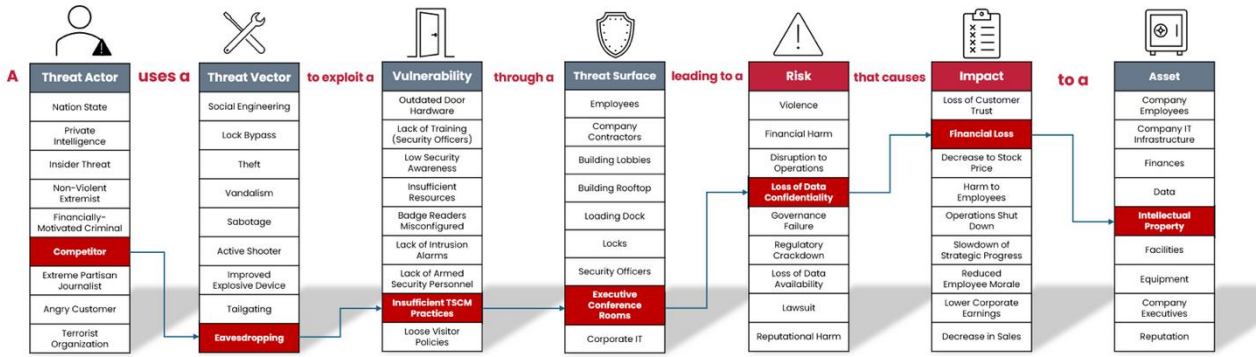
Steps:

1. Threat Model
2. Gather Buy-In
3. Scope
4. Propose
5. Prepare
6. Practice
7. Execute
8. Immediate Deescalation
9. Report
10. Follow Up

Model Your Threats

Determine your Attacker, Vector, and Surface



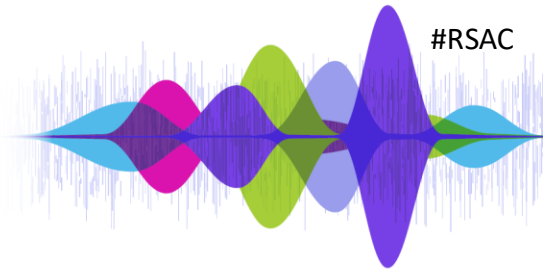


Listen and Talk

Determine your Need-to-Know

Gathering Buy-In:

1. Pre-Work: Have a reputation as a collaborative partner
2. Meet with security leaders and listen
    a. Understand their pain points, known vulnerabilities, and worry areas
3. Discuss what red teaming is and how red teams can help
4. Do not pitch yet.
5. Leave with promise of a follow up and proposal for an op that supports their needs



Scope Your Engagement

Create a safe and realistic scope

Scope your Engagement:

1. What is the goal?
   a. Primary
   b. Secondary / Unstated
2. Name the Operation
3. What type of test?
4. What are the risks you need to consider?
5. Where are you testing? Be specific.
6. When are you testing? Be specific.
7. What are you testing? Be specific.
8. How are you testing? Be specific.

Scope your Engagement:

1. Who is approving the test?
   a. Do they have authority to approve?

Resource

Scoping Checklist

Propose Your Engagement

Develop your OpsProposal

Proposing:

1. Use what you Learned (Speak to Audience)
    a. Document Scope Thoroughly
2. Address Risks Proactively
    a. Establish Safeguards
3. Don't Finalize, but Prepare
4. Develop your Communications Plan
    a. Include "Who Shouldn't Know"
5. Present / Send to Leadership (As Needed)
    a. Do Proposal Regardless
6. Living Document - Until Finalized

Resource

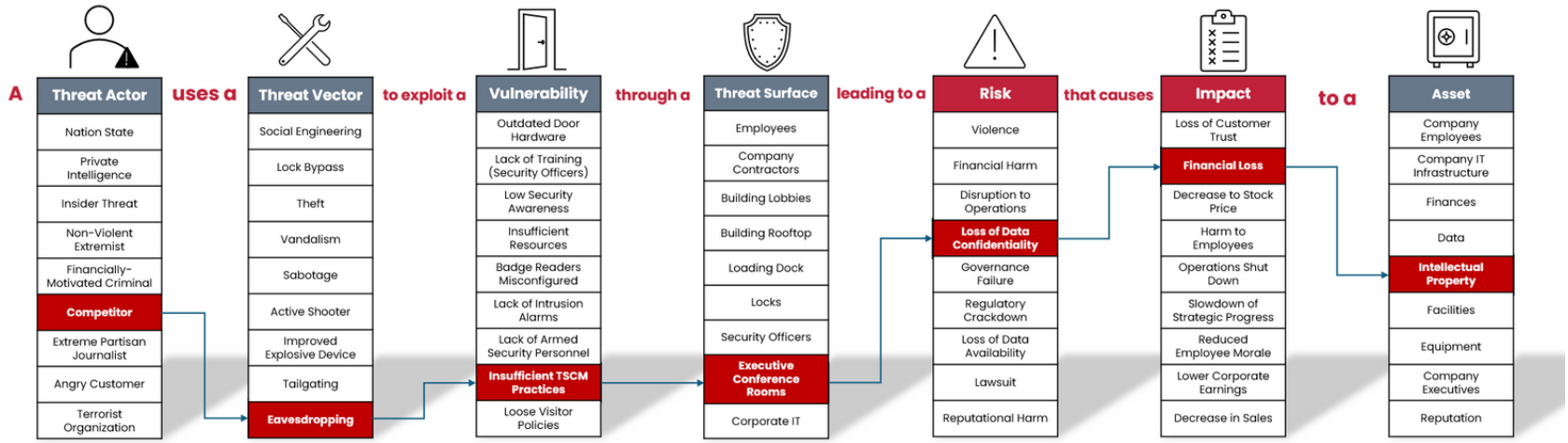
Physical Proposal/OpsPlan

Ops Proposal

Red Team Operation Proposal

Include:

- Threat Model
  - Adversary
  - Motivation
  - Tools & Tactics
  - Target(s)



Prepare For Your Operation

Create a safe and realistic scope

Prepare for Go-Time:

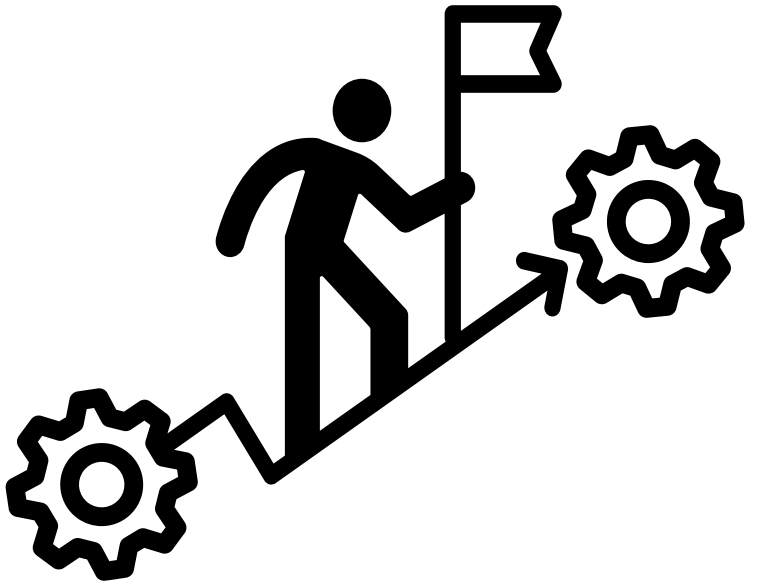
1. Develop an OpsPlan
    a. Converted Proposal
    b. Less Justification
    c. More Operational Details
2. Gather Resources
3. Final Sign-Offs
4. Admin Work

Practice Your TTPs

Get Hands-On

Practice:

1. Red Team your Red Team
    a. Pre-Mortem Analysis
2. Practice Tools, Tactics, Procedures
3. Adjust as Needed



Execute Your Operation

GO GO GO!

Putting the ACT in Practice:

1. Follow Scope
2. Think on your Feet
3. Communicate Well
    a. Within the Team
    b. With Leadership
4. Know When to Stop
    a. Gather Useful Data
5. Communicate the STOPOP
    a. Internally (Get Confirmation)
    b. Externally

Immediate Debrief & De-escalation

SLOW SLOW SLOW!

Debrief:

1. Within an Hour of STOPOP
2. Stop Rumors
3. Talk to Social Engineering Victims
    a. Explain and Ask “What would have…”
4. Be Everyone’s Friend
5. Do Root-Cause Analysis
6. Immediately Praise/Reward Champions
7. Gather Data/Perspective While It’s Fresh
8. Record Voice Memos

Report Your Results

Present your Findings

Communicate your Findings:

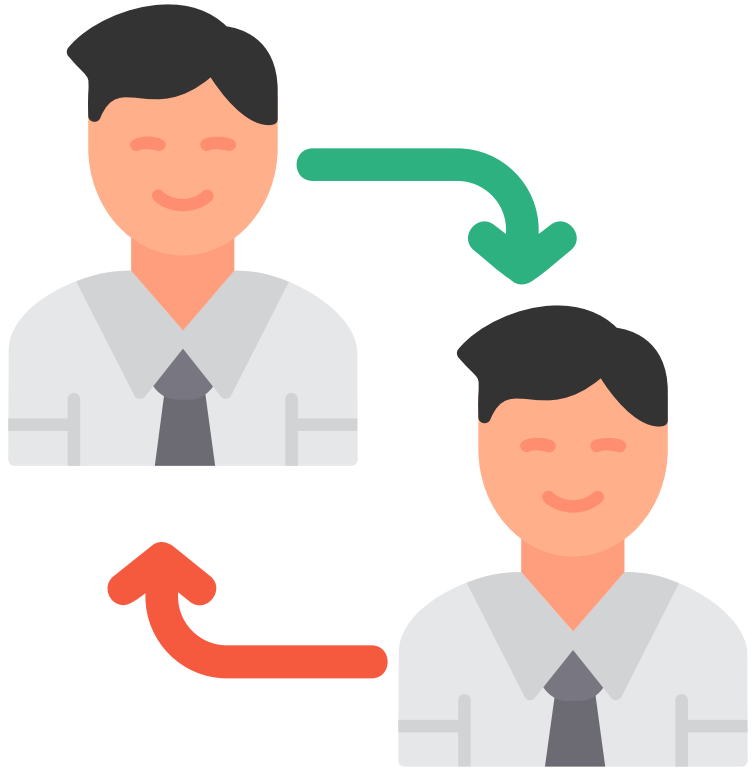
1. Presentations
    a. Show & Tell
2. Reports
    a. Include Everything
    b. Draft Executive Summary
3. Registers
4. Tasks
5. Meetings
    a. “Meeting Chicken”

Follow Up with Your Partners

FU - no FU!

Keep Momentum:

1. Highlight Positive Changes
    a. They Look Good
    b. You Look Good
    c. Security Gets Better
2. Retest as Needed
    a. Ad-Hoc; or
    b. Project Management Check-Ins
3. Use a Dashboard
    a. If You're an Overachiever
4. **Promote Positive Change**



RSAC 2025 Conference

Mitigating the Uncovered Risks

Towards Purple Teaming

Mitigating Findings

Fixing the Vulnerabilities Uncovered by the Red Team

Be Creative:

1. Cheap
    a. Gamify Security
    b. Improve the Culture
    c. Leverage Allies
2. Easy
    a. Reward Good Behavior
    b. Be Transparent
3. Effective
    a. Upgrade Systems Strategically
    b. Take Big Bets

VERIFIED OSDP™ VERIFIED

RSAC 2025 Conference

Many Voices.
One Community.

Get in Touch:

Text/Call: (628) 777-7475
Signal: (952) 465-4769

Shawn@PineRisk.com
Ana@PineRisk.com

Reddit.com/r/PhysicalRedTeam
Discord:ByteAbel
LinkedIn.com/Company/PineRisk